

REMARKS

Claims 1-12 are all the claims pending in the application. By this amendment, Applicant editorially amends claims 1-3, 6, 7, 9, and 12 to clarify the invention and to fix minor informalities. In particular, claims 2, 3, 6, and 7 are not amended for reasons related to patentability.

Preliminary Matters

Applicant thanks the Examiner for initialing the references listed on Form PTO-1449 submitted with the Information Disclosure Statement on May 7, 2001. Applicant also thanks the Examiner for accepting the drawings filed on March 12, 2001 and for acknowledging the claim to foreign priority and for confirming that the certified copy of the priority document was received.

Claims Rejected under 35 U.S.C. § 102

Claims 1-12 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 4,912,310 B1 to Uemura et al. (hereinafter "Uemura"). Applicant respectfully traverses this rejection and respectfully requests the Examiner to reconsider in view of the following comments.

Of the rejected claims, only claims 1, 9, and 12 are independent. This response, at least initially, focuses on these independent claims. First, independent claim 1, among a number of unique features, recites: "in case said authentication process was successful, carrying out a software operation by said first system device, by which software operation said encryption key stored in said first user device is replaced by a second encryption key, wherein said second encryption key is stored in second system devices and further user devices used in a second level

of said key and lock system, thereby making said user device operable with said second system and further user devices.” The Examiner alleges that claim 1 is directed to a method of authorizing a user device of a key and lock system and is anticipated by the teachings of Uemura. The Examiner asserts that when an authentication process was successful, a software operation is carried out by the first system device, by which software operation the first encryption key stored in the user device is replaced by a second encryption key as set forth in claim 1 is equivalent to a card issuing machine issuing a first card and using this card as a key for issuing another card of lower level as described in col. 3, lines 10 to 18 and lines 31 to 32 of Uemura (see page 3 of the office action). Applicant respectfully disagrees with the Examiner. Applicant has carefully studied Uemura’s discussion of the card issuing machine issuing a card, which is not similar to having one single user device provided with variable encryption key as set forth in claim 1.

For example, in the exemplary, non-limiting embodiment of the present invention, by providing an encryption key in a user device, which can be a key or a lock of a key and lock system, high security is achieved. At different levels *i.e.*, manufacturer, distributor, and customer level, this encryption key is changed by using a system device of the respective level. Thereby, one single user device is provided with a variable encryption key. This passage is provided by way of an example only and is not intended to limit the scope of the claims in any way.

Uemura, on the other hand, discloses a method of issuing cards by using a card issuing machine including a memory having stored therein an initial secret code, a card reader, and a keyboard. In Uemura, this initial secret code is keyed in and upon a match, a new secret code is keyed in for associating a first card with the card issuing machine (*see* Abstract). In particular,

Uemura teaches the first card is issued by the card issuing machine on condition that the secret code keyed-in matches the initial secret code stored in the memory of the machine. At this time, a code for associating the first card with the card issuing machine is keyed in and stored in the first card and in the machine. With the issue of the first card, the first card is closely associated with the issuing machine. The first card is of the highest level and serves as a key for issuing another card of lower level. The first secret code as to the first card is stored in the memory of the issuing machine. If the issuer of the first card differs from the person who registers the first secret code of the first card issued in the issuing machine, the issuer of the first card can no longer participate in the subsequent issue of cards. Accordingly, Uemura teaches a hierarchical card system because a card of low level can be issued only by using a card of higher level (col. 3, lines 10 to 44).

Uemura, however, is very different from the method set forth in claim 1. Uemura can be thought of as antithesis of the method in claim 1. In Uemura, the secret code is used to associate a card with one card issuing machine. That is, Uemura stores secret codes in the card issuing machine and the cards. No stored codes are replaced by other codes. The purpose of storing the codes in both the card issuing machine and the cards is to associate a card with the card issuing machine (cols. 13 and 14).

In Uemura, an authorization card is inserted into the card issuing machine and the data on the card is read. Upon a match between the secret code stored in the machine and the code stored in the card, the secret code is entered by the user and, depending on authorization level, a desired operation is selected. In Uemura, however, the secret code stored in the card cannot be changed as there would be no match between the code stored in the machine and the code stored

in the card. In short, Uemura fails to teach or suggest replacing the encryption key such that once the change in the encryption key has taken place, the user device is no longer associated with the first system devices.

In addition, Uemura uses secret codes, *i.e.*, identifications that are keyed in and stored in the card issuing machine and the cards. Uemura's identifications are used for identifying devices and not for further communication between devices. That is, Uemura fails to teach or suggest the encryption keys being used for further communication between different devices. Moreover, Uemura teaches a method of issuing cards, and not distributing cards between different hierarchical levels, such as a manufacturer, a locksmith, and an end user. Uemura describes the use of the method within a hotel, wherein either authorization cards or guest cards are issued. In short, Uemura fails to teach or suggest changing encryption key to attain the secure distribution of keys and in this process of changing the encryption key of a user device having no new device being issued.

Therefore, "in case said authentication process was successful, carrying out a software operation by said first system device, by which software operation said encryption key stored in said first user device is replaced by a second encryption key, wherein said second encryption key is stored in second system devices and further user devices used in a second level of said key and lock system, thereby making said user device operable with said second system and further user devices," as set forth in claim 1 is not taught by Uemura. Uemura lacks having stored codes being replaced by other codes, having the cards for further communication between different devices, and distributing the cards between different hierarchical levels. For at least these exemplary reasons, claim 1 is patentably distinguishable from Uemura. Therefore, Applicant

respectfully requests the Examiner to withdraw this rejection of claim 1. Claims 2-8 are patentable at least by virtue of their dependency on claim 1.

Claims 9 and 12 recite features similar to the features argued above with respect to claim 1. Therefore, arguments presented with respect to claim 1 are respectfully submitted to apply with equal force here. Applicant therefore respectfully requests the Examiner to withdraw this rejection of independent claims 9 and 12. Also, Applicant respectfully submits that claims 10 and 11 are allowable at least by virtue of their dependency on claim 9.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

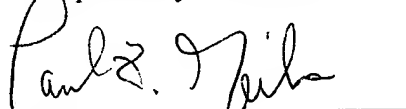
WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Date: December 27, 2004

Respectfully submitted,



Paul F. Neils
Registration No. 33,102